Continuation of Application for Search Warrant

Based on my knowledge, training and experience, and the investigation of law enforcement officers with personal knowledge and with whom I am working, I, Alexis Giudice, being duly sworn, depose and state as follows:

INTRODUCTION

1. Based on the information set forth below, there is probable cause to believe that evidence of violations of federal law, specifically, Title 21, United States Code, Sections 841(a)(1) and 846 [Possession with Intent to Distribute Controlled Substances, and Drug Trafficking Conspiracy] will be found on certain electronic devices (hereinafter the "**Subject Devices**," described more fully in Attachment A). The categories of electronically stored information and evidence sought are described in Attachment B.

2. This Application requests the issuance of a warrant to examine the **Subject Devices** that were seized on August 19, 2020, following the execution of a federal search warrant on August 19, 2020, and the arrest of JAMES KUYKENDOLL SR.

APPLICANT'S TRAINING AND EXPERIENCE

3. I am a Special Agent with the Drug Enforcement Administration ("DEA"), a position I have held since approximately August 2015. As part of my duties, I investigate criminal violations of the federal drug trafficking laws. I have been involved with various electronic surveillance methods, the debriefing of defendants, informants, and witnesses, as well as others who have knowledge of the

distribution, transportation, storage, and importation of controlled substances. I have received training in the area of drug investigations, money laundering, financial investigations, and various methods which drug dealers use in an effort to conceal and launder the proceeds of their illicit drug trafficking enterprises. I have participated in investigations that have led to the issuance of search warrants involving violations of drug laws. These warrants involved the search of locations including: residences of targets, their associates, and relatives; storage facilities; smartphones; and computers. Evidence searched for, and recovered, in these locations has included controlled substances, records pertaining to the expenditures and profits realized therefrom, monetary instruments, and various assets that were purchased with the proceeds of the drug trafficking.

4. I also know from training and experience that drug traffickers frequently utilize mobile telephones and other electronic devices, such as tablets and laptop and desktop computers, to facilitate drug trafficking. Mobile telephones are portable, and some mobile telecommunications service providers do not require purchasers of the devices to provide their names and/or addresses, so narcotics traffickers often use the devices in an effort to avoid detection by law enforcement. Mobile phones often contain evidence indicative of drug trafficking, including records of incoming and outgoing calls and text messages with suppliers of narcotics; voicemail messages; photographs of drugs, coconspirators, or currency; and, in the case of "smart phones," Global Positioning System (GPS) data indicating the location of the device at given points in time, providing evidence that the device was in high

drug trafficking areas or evidencing the route used in trafficking narcotics. Additionally, drug traffickers typically maintain and use multiple mobile phones to facilitate sales, and frequently switch phones to evade detection by law enforcement. Further, these types of devices are frequently used to access social media websites such as Facebook, Instagram, etc. In my training and experience, drug traffickers are using social media with increasing frequency to communicate with suppliers and purchasers of narcotics.

5. Similarly, I also know from training and experience that drug traffickers use tablets, laptop and desktop computers to further their activities by, for example, producing and maintaining drug ledgers and other financial records, photos/videos of drug trafficking and/or associates, and other related digital files. Storing this information can be intentional by the user, such as saving an e-mail as a file on the computer or tablet or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally without the user's specific knowledge. This might include traces of the path of an electronic communication being automatically stored in many places, such as temporary files or Internet service provider (ISP) client software, or files that were previously viewed or deleted being retained in "free disk" space. In addition to electronic communications, a computer or tablets user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains certain file sharing software, when the computer was sharing files, and some of the files

which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

6. I also know from training and experience that drug traffickers utilize cameras and video cameras to take photos/video of narcotics, currency, high value items and coconspirators.

PROBABLE CAUSE

7. Since September 2019, DEA Grand Rapids, DEA Chicago, the Grand Rapids Police Department, the Kent Area Narcotics Enforcement Team and the Michigan State Police have been conducting this joint investigation into the drug trafficking activities of the KUYKENDOLL Drug Trafficking Organization ("KUYKENDOLL DTO"), which includes but is not limited to DTO heads JAMES KUYKENDOLL SR and JAMES KUYKENDOLL JR, MARNELL DAVIS, ADONNAS BROWN, DEREK KUYKENDOLL, KYLE PARISH, ELIJAH ALLEN, ANGELICA ENRIQUEZ and KEVIN FENSKE.

8. Based on physical and electronic surveillance and information provided by a DEA Confidential Source, the KUYKENDOLL DTO has an unknown source of supply located in Chicago, Illinois for heroin/fentanyl. The KUYKENDOLL DTO provides bulk cash to the unknown source of supply in Chicago, Illinois in exchange for the narcotics.

9. Over the course of the investigation, a KANET Confidential Source[1] has purchased cocaine from JAMES KUYKENDOLL SR on numerous occasions. During the course of the controlled purchases, the transactions were coordinated via cellular communication devices.

10. For example, on November 18, 2019, investigators met with the KANET CS and observed the KANET CS place a phone call the JAMES KUYKENDOLL SR and request cocaine. JAMES KUYKENDOLL SR instructed the KANET CS to meet KUYKENDOLL SR in the area of 28th ST SW/Clyde Park Ave. The KANET CS was then searched for contraband by investigators, which resulted in negative results. Investigators established surveillance in the area of 28th ST SW/Clyde Park Ave SW, in Wyoming, Michigan in order to conduct surveillance of a meeting between a KANET CS and JAMES KUYKENDOLL SR. Investigators then followed the KANET CS to the pre-determined meet location and observed the KANET CS enter Roger's Plaza. Investigators then observed JAMES KUYKENDOLL SR enter Roger's Plaza and meet with the KANET CS.

11. Investigators then followed the KANET CS to a pre-determined meet location to debrief with agents. The KANET CS immediately produced one plastic bag containing cocaine. A field test of the cocaine resulted in a positive result. The

[1] The CS' criminal history included: State of Michigan convictions for drugs and traffic offenses. The CS is cooperating as a defendant and has a pending criminal charges. The information that the CS provided in the interview was corroborated through the on-going investigation, statements provided by other cooperating sources, and information obtained via physical surveillance and search of law enforcement databases. Based on the foregoing, this source is credible and reliable.

KANET CS was then searched again for contraband, which resulted in negative results.

12. On December 21, 2019, a federal search warrant was executed on KUYKENDOLL SR's residence located at 908 Four Mile Road, APT 2A, Grand Rapids, Michigan, which resulted in the seizure of approximately $5,850 US currency, a hand press, 2 digital scales, 4 cell phones and approximately 40.2 grams of heroin.

13. In the week following the execution of the search warrant, KUYKENDOLL SR made contact with investigators and advised he wanted to cooperate with law enforcement. Following this meeting, KUYKENDOLL SR kept in limited contact with DEA Grand Rapids for about 3 weeks before ultimately ending all contact with law enforcement. KUYKENDOLL SR did not respond to further phone calls and text messages by law enforcement to attempt to further his cooperation.

14. On February 26, 2020, the Honorable Judge Paul Maloney authorized a federal arrest warrant for JAMES KUYKENDOLL SR for Possession with Intent to Distribute Controlled Substances and Possession with Intent to Distribute Heroin.

15. On August 18, 2020, the Honorable Judge Ray Kent authorized a federal GPS ping warrant on phone number 630-589-2699, which was identified as a phone number belonging to KUYKENDOLL SR.

16. On August 19, 2020, DEA Chicago and the USMS Chicago located JAMES KUYKENDOLL SR in Chicago, Illinois at 422 N St. Louis Ave, Chicago, Illinois. KUYKENDOLL SR was arrested pursuant to the federal arrest warrant.

17. On August 19, 2020, a federal GPS ping revealed KUYKENDOLL SR's phone to be located within 422 N St. Louis Ave, Chicago, Illinois. Based on this phone ping data, investigators believed KUYKENDOLL SR to be within the residence. Members of DEA Chicago and USMS Chicago knocked on the front door of the residence. A female answered the door and advised law enforcement that she lived there. Law enforcement asked the female if KUYKENDOLL SR was in the house and the female informed law enforcement that KUYKENDOLL SR was upstairs. Law enforcement asked for consent to make entry into the residence to arrest KUYKENDOLL SR and the female gave consent. While clearing the upstairs for their safety, DEA Chicago observed a white IPhone 6 Plus in plain view in a bedroom identified as belonging to KUYKENDOLL SR. DEA Chicago also found KUYKENDOLL SR upstairs and placed him under arrest. DEA Chicago located a white IPhone 6 in KUYKENDOLL SR's front right pocket Investigators also located a digital scale sitting on the kitchen table of the residence. Based on my training and experience, the ongoing investigation, I believe that KUYKENDOLL SR has continued his narcotics related activities in Chicago, Illinois.

18. Based on the information set forth above, the physical evidence seized and my knowledge, training and experience in drug trafficking investigations, I respectfully submit there is probable cause to believe additional evidence of drug

trafficking will be found in electronic format on the **Subject Devices**. Based on the totality of the circumstances discussed above, there is probable cause to believe that those **Subject Devices** will contain contact lists, telephone logs, photographs and other data that relate to drug trafficking.

19. The **Subjects Devices** are more specifically described as the following devices that are currently in the custody of DEA Grand Rapids that were seized from 422 North St. Louis Ave, Chicago, Illinois on August 19, 2020:

a. A White IPhone 6

b. A White IPhone 6 Plus

20. The **Subject Devices** were initially seized by DEA Chicago and turned over to DEA Grand Rapids. The **Subject Devices** have been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as they were when the **Subject Devices** were first seized by DEA Chicago on August 19, 2020.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. The warrant applied for would authorize the extraction and copying of electronically stored information, all under Rule 41(e)(2)(B).

a. Based on my knowledge, training, and experience, I know that cell phone files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be

recovered months or years later using forensic tools. This is so because when a person "deletes" a file, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, a cell phone's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, cell phone storage contains electronic evidence of how the cell phone has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. cell phone users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Based on my training and experience, I am aware that cell phone equipment is almost always used to plan and communicate actions within a narcotics distribution conspiracy.

22. As further described in Attachment B to the Search Warrant Application for the **Subject Devices**, this application seeks permission to locate not only cell phone files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, the purpose of their use, who used them, and when.

23. Although some of the records called for by this warrant might be found in the form of user-generated files, cell phone storage media can contain other forms of electronic evidence as well:

a. Forensic evidence of how cell phones were used, the purpose of their use, who used them, and when, is specifically described in Attachment B to the Search Warrant Application for all target locations. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record

additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Cell phone file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a cell phone or storage medium can also indicate who has used or controlled the cell phone or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the cell phone or storage medium at a relevant time.

c. A person with appropriate familiarity with how a cell phone works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance with particularity a description of the records to be sought, evidence of this type often is not always data that can be merely reviewed by a review

team and passed along to investigators. Whether data stored on a cell phone is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

e. Further, in finding evidence of how a cell phone was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a cell phone, often without the cell phone user's knowledge, that can allow the cell phone to be used by others, sometimes without the knowledge of the cell phone owner. Also, the presence or absence of counter-forensic programs (and associated data) that are designed to eliminate data may be relevant to establishing the user's intent. To investigate the crimes described in this warrant, it might be necessary to investigate whether any such malicious software is present, and, if so, whether the presence of that malicious software might explain the presence of other things found on the storage medium. I mention the possible existence of malicious software as a theoretical possibility, only; I will not know, until a forensic analysis is conducted, whether malicious software is present in this case.

f. Searching storage media for the evidence described in the attachments may require a range of data analysis techniques. It is possible that the storage

media located on the premises will contain files and information that are not called for by the warrant. In rare cases, when circumstances permit, it is possible to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, it is possible, though rare, for a storage medium to be organized in a way where the location of all things called for by the warrant are immediately apparent. In most cases, however, such techniques may not yield the evidence described in the warrant. For example, information regarding user attribution or Internet use is located in various operating system log files that are not easily located or reviewed. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

24. Authority is sought to utilize the services of outside cell phone experts, who may not be federal law enforcement officers, in order to use and operate the computer system(s) at the above specified locations for purposes of retrieving the above specified computer information during the course of the authorized search, provided that such experts operate under the direction, supervision, and control of the Special Agents in charge of this case.

CONCLUSION

25. I respectfully submit that there is probable cause to believe that JAMES KUYKENDOLL SR has engaged in the distribution of, and in the possession with intent to distribute cocaine, and that they have conspired to do the same, in violation of 21 U.S.C §§ 841 and 846. I submit that this application supplies probable cause for a search warrant authorizing the examination of the **Subject Devices** described in Attachment A to seek the items described in Attachment B.